"Detained at the Border: Electronic Device Searches, Biometrics, and Policy Continuity (2001–2025)"

Independent Observer Vol II

Abstract

This working paper explains the U.S. ***"border search"*** doctrine as it applies to U.S. citizens and **lawful permanent residents (green card holders)**, with a particular focus on electronic device searches and facial biometric programs at ports of entry. Drawing on Supreme Court precedents (**e.g., Ramsey, Montoya de Hernandez, Flores–Montano**), recent circuit decisions (**Cotterman, Cano, Alasaad**), as well as DHS/CBP directives and statistics, we outline what officers can lawfully do, what requires heightened suspicion, and how policies have evolved across four administrations. We demonstrate that, although public rhetoric has become, core authorities—such as warrantless "basic" device searches at the border, thresholds for prolonged detention, and the rapid adoption of facial comparison—have essentially remained unchanged—**title 42 public-health** expulsions ended on **May 11, 2023**, with processing returning to Title 8. Policy options include standardized auditing of "advanced" device searches, more precise limits on data retention and sharing, and consistent notice and opt-out procedures for biometrics.

Keywords

Border search exception; electronic devices; biometrics; facial recognition; lawful permanent residents; Fourth Amendment; DHS/CBP policy.

JEL / Subject Areas

K14 (Criminal Procedure); K38 (Human Rights Law); H11 (Government Structure).

Disclosure

Nothing to disclose.

Rights

Method and Scope

> Legal–policy synthesis of constitutional doctrine, circuit splits, and official DHS/CBP guidance. Focus on electronic devices and biometric verification at U.S. ports of entry across the administrations of Bush, Obama, Trump, and Biden. Not individualized legal advice.

1. Legal Framework: The Border Search Exception

The Supreme Court has long recognized warrantless searches at the international border as "reasonable" under the Fourth Amendment: United States v. Ramsey (431 U.S. 606, 1977). For detentions exceeding a routine customs inspection, reasonable suspicion is necessary **(United States v. Montoya de Hernandez, 473 U.S. 531, 1985)**. Vehicle disassembly, such as removing a gas tank, does not require reasonable suspicion (United States v. Flores–Montano, 541 U.S. 149, 2004).

Constitutional baseline and statutory authority. The Supreme Court has consistently held that searches at the international border (and its functional equivalents) are "reasonable" under the Fourth Amendment, simply because of their location, allowing warrantless inspections separate from ordinary domestic policing. Congress and relevant agencies codify this in customs and immigration statutes and regulations—e.g., 19 U.S.C.

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.

§§ 1581–1582 (customs boarding and searches), 8 U.S.C. § 1357 (immigration officers' powers), and 19 C.F.R. § 162.6 (search of persons, baggage, and merchandise). United States v. Ramsey establishes the constitutional baseline: border searches conducted without a warrant or probable cause are still considered reasonable.

1.2 Where the exception applies (border, "functional equivalent," and checkpoints). The Court permits brief, suspicionless stops at fixed checkpoints near the border (Martinez-Fuerte v. California). Still, it forbids suspicionless vehicle searches at interior checkpoints away from the border or its functional equivalent (Ortiz). Roving patrol stops require reasonable suspicion (Brignoni-Ponce). Together, these cases mark the line between actual border/functional-equivalent settings (e.g., an international airport gate) and interior enforcement where ordinary Fourth Amendment limits reassert themselves. Legal Information InstituteJustia Law+2Justia Law+2

1.3 Persons vs. property; "routine" vs. "non-routine." Intrusive searches of the person at the border demand at least reasonable suspicion (e.g., alimentary-canal smuggling detention in Montoya de Hernandez), while routine inspections of effects and conveyances are broadly permissible—up to and including disassembly that is not destructive (Flores-Montano upheld removal of a gas tank without suspicion). This "person/property" and "routine/non-routine" distinction drives much of the modern analysis. Justia Law+1

1.4 Electronic devices: doctrine and split. For digital devices, courts distinguish between a **basic/manual** review and an **advanced/forensic** examination. CBP Directive 3340-049A (Jan. 2018; page updated June 18, 2025) formalizes this operationally and ties advanced searches to reasonable-suspicion or national-security predicates. Appellate rulings diverge: the Ninth Circuit requires reasonable suspicion for forensic device searches and limits their **scope** to digital contraband (Cotterman; Cano); the Fourth Circuit requires at least individualized suspicion for forensic analysis (Kolsuz); the Eleventh Circuit permits forensic searches without any suspicion (Touset); and the First Circuit (Alasaad) held no warrant or probable cause is required and allowed basic searches without suspicion while accepting agency policy on advanced searches. Riley v. California (not a border case) underscores the heightened privacy interests in phones and informs the reasoning of several circuits. U.S. Customs and Border Protection+1Ninth Circuit Court of Appeals+2Ninth Circuit Court of Appeals+2Justia Law+2Justia Law+2Eleventh Circuit Court of AppealsUS Courts MediaJustia Law

1.5 Key takeaways for this report. (i) At true borders and functional equivalents, warrantless inspections remain the norm, constrained by the person/property and routine/non-routine lines; (ii) digital forensics are the live area of dispute, with circuits split on the suspicion threshold and search scope; and (iii) agency policy (CBP 3340-049A) and local precedent together dictate the practical standard a traveler will encounter at a given port. U.S. Customs and Border ProtectionUS Courts Media

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.

2. Electronic Devices: "Basic" vs. "Advanced" Searches

CBP Directive 3340-049A regulates the search of electronic devices. A "basic" search involves a manual review by an officer, while an "advanced" search uses external equipment to review, copy, or analyze data. Advanced searches require supervisory approval and involve specific facts related to national security, immigration, or customs concerns. Courts differ: the Ninth Circuit requires reasonable suspicion for forensic examinations (**United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013)** (en banc)) and limits warrantless searches of digital contraband to those involving phone searches **(United States v. Cano, 934 F.3d 1002 (9th Cir. 2019)**). The First Circuit permits suspicionless "basic" device searches (Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021).

2.1 What CBP policies say.

CBP's controlling directive draws a bright operational line. A **basic search** is any device inspection that is not "advanced" and generally means a manual review of content resident on the device. An **advanced search** connects external equipment to "review, copy, and/or analyze" contents. It may occur only with (i) **reasonable suspicion** of a law violation enforced or administered by CBP **or** a **national security concern**, and (ii) **supervisory approval** at GS-14 (or equivalent) or higher. Before conducting either type of search, officers must **disable network connectivity** and refrain **from intentionally accessing information that is solely stored remotely** (i.e., cloud-only data).CBP's public summary tracks those definitions and reiterates that advanced searches require suspicion or a national-security predicate with senior approval.

2.2 Legal thresholds and the current split.

Courts agree that brief, manual "basic" reviews are easier for the government to justify under the border-search exception but differ on **forensic** (advanced) extractions. The Ninth Circuit requires **reasonable suspicion** and limits the **scope** of border phone searches—manual or forensic—to **digital contraband** (e.g., child sexual abuse material), not a broad search for general evidence. The Ninth Circuit Court of Appeals and the Fourth Circuit similarly require at least individualized suspicion for a forensic phone search. ca4.uscourts.govanticorruptionblog.com The Eleventh Circuit, by contrast, allows forensic device searches **without any suspicion**. The First Circuit (Alasaad) rejected a warrant requirement, accepted agency policy that links advanced searches to reasonable suspicion or national-security concerns, and permitted **basic** searches without suspicion. US Courts MediaHarvard Law Review Although not a border case, the Supreme Court's decision in **Riley v. California** highlights why many courts view digital extractions as highly intrusive: phones reveal the "privacies of life," which influences border analysis even though Riley's arrest-search rule does not apply.

2.3 Passcodes, detention, and documentation.

Travelers must present devices "in a condition that allows inspection." Officers may request **passcodes** (retained only as needed for the search and then **deleted/destroyed**). They may **detain** a device for a "brief, reasonable" period to complete the search—**ordinarily not to exceed five (5) days**, with documented supervisory extensions and, beyond 15 days, higher-level approvals. CBP must provide a

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.

custody receipt (Form 6051D) when a device is held. Searches and detentions must be documented in CBP systems (TECS / Electronic Media Report).

2.4 Special categories and remote data.

Attorney-client, work-product, medical, journalistic, and business-confidential materials trigger **segregation and counsel-coordination** procedures; copies of privileged material are destroyed after review unless retained solely to meet a legal hold. Separately, CBP policy prohibits the **intentional access of cloud-only content** and requires airplane mode or connection-off procedures to enforce this limit.

2.5 Practical takeaways.

In practice: (i) **basic** = manual, on-device review; no suspicion required by policy, though local precedent may narrow scope (e.g., Ninth Circuit). (ii) **advanced** = external-tool forensic work; requires **reasonable suspicion or a national-security concern** plus **GS-14** approval. (iii) Officers should **disable connectivity** and avoid cloud-only data; (iv) passcodes can be requested but must be purged after use; (v) devices can be **detained briefly** with a receipt and logged in TECS; (vi) **privileged/sensitive** materials get special handling. Travelers' actual exposure, therefore, turns on **circuit** and **port-level practice**, with CBP's policy setting the floor and cases like *Cotterman*, *Cano*, *Kolsuz*, *Touset*, and *Alasaad* defining the ceiling by region.

3. Programmatic Evolution Across Four Administrations (2001–2025)

3.1 2001–2008 (Bush). After 9/11, DHS launched the US-VISIT program to collect biometrics from most arriving foreign nationals at air and seaports, including digital photos and fingerprints, formalized in a January 5, 2004, Federal Register rule. US-VISIT's goal established the framework still used by CBP for identity operations: screening against watchlists, verifying identities, and recording arrivals and departures. By 2006, CBP's Automated Targeting System (ATS) had a published Privacy Impact Assessment (PIA) describing rule-managed risk scoring for traveler and cargo data—an early version of today's pre-screening processes. In 2007–2008, DHS upgraded from **two-print** to **ten-print** fingerprint enrollment and began deploying 10-print scanners at ports of entry, completing the nationwide rollout by the end of 2008. US-VISIT's biometric strategy and oversight challenges during this period were tracked by the U.S. Department of Homeland Security and the Government Accountability Office, highlighting how identity operations became a permanent border function.

3.2 2009–2016 (Obama).

CBP issued its first dedicated **Border Search of Electronic Devices** directive on August 20, 2009 (Directive **3340-049**), standardizing practices for "basic" review, advanced examinations, retention, and sharing. U.S. Department of Homeland Security. In 2013, DHS established the Office of Biometric Identity Management (**OBIM**) to replace US-VISIT and operate IDENT, which is now the core DHS biometric repository for immigration and border missions. In the final years of the administration, CBP launched biometric **exit** pilots: the **Departure Information Systems Test (DIST)** and related field tests (e.g., Atlanta jetway photo-matching in June 2016), documented in a

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.

December 2016 PIA and subsequent GAO reports. These pilots demonstrated the practicality of using facial recognition for high-throughput identity checks at the gate. U.S. Customs and Border Protection.

3.3 2017–2020 (Trump).

CBP updated its device-search policy with **Directive 3340-049A** (January 4, 2018), along with an accompanying PIA addressing privacy risks related to modern device examinations. U.S. Department of Homeland Security+1 In parallel, CBP implemented what is now known as the **Traveler Verification Service (TVS)**—a facial comparison service used across air, land, and sea—building on the 2016 pilots and early 2017 deployments at Dulles, O'Hare, and other airports. U.S. Department of Homeland Security, U.S. Customs and Border Protection. Federal rulemaking and oversight materials from 2020 explicitly connect current biometric entry-exit plans to those from 2016 facial recognition pilots. During this period, appellate courts clarified the **distinction between basic and advanced** device searches. The Ninth Circuit required **reasonable suspicion** for forensic searches (Cotterman; Cano), whereas other circuits adopted more deferential views toward the government.

3.4 2021–2025 (Biden).

Programmatically, CBP emphasized transparency metrics and scaled facial comparison nationwide. In FY2023, CBP reported processing **over 172 million** travelers with facial comparison, achieving a match rate of over 98%; a total of **394** million travelers were processed overall at ports of entry. U.S. Customs and Border Protection CBP's FY2024 device-search statistics quantify 47,047 BSEDs—about 0.3% of secondary inspections and <0.01% of all arrivals—and provide a detailed basic/advanced and citizenship breakdown. U.S. Customs and Border Protection +1 GAO's 2022 review shows that FRT is deployed across air, sea, and land modalities, reflecting TVS's maturation beyond aviation. U.S. Government Accountability Office On the legal front, district-level rulings (e.g., EDNY, July 29, 2024) have begun to press stricter standards in specific jurisdictions, while the CBP directive page itself (3340-049A) shows continued policy maintenance (page updated June 18, 2025). The Verge U.S. Customs and Border Protection. Recent reporting also notes a record quarterly volume of device searches in Q2 2025, consistent with CBP's longer-term trend data. (Use press figures with caution and anchor formal counts to CBP's FY summaries.) WIRED

Synthesis. Across administrations, a consistent theme has emerged: institutionalization, with identity and device-search authorities based on longstanding border doctrine, gradually formalized through directives (2009, 2018), privacy documentation (ATS/TVS PIAs), and public statistics (FY 2023–FY 2024). The technical infrastructure shifted from fingerprint-only systems (US-VISIT) to cloud-based facial comparison (TVS). Simultaneously, courts refined the evidentiary threshold for advanced device searches without eliminating the core border search exception. U.S. Department of Homeland Security+2

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.

4. Biometrics at Ports of Entry

CBP's Traveler Verification Service supports facial comparison at air, land, and seaports. CBP provides reports on nationwide deployments, retention limits (such as briefly holding U.S. citizen photos for operational purposes), and opt-out signage; collaboration with TSA and carriers increases usage. 4. Biometrics at Ports of Entry — Extended 4.1 Operational Model (TVS). CBP's Traveler Verification Service (TVS) allows quick facial comparisons at airports, land crossings, and seaports through integration with carriers and TSA. Agency materials describe nationwide deployments, short-term retention of U.S. citizen photos for operational needs, and posted opt-out options where available (manual inspection replaces face capture if declined). These integrations explain why travelers now see facial capture not only during primary inspection but also at boarding and exit gates. 4.3 Risk and Accountability. Claims about accuracy depend on the audits supporting them. False positives (misidentifications) cause delays and extra inspection costs; false negatives (missed matches) lead to security rework. The limited transparency about algorithm performance and human-in-the-loop override rates is why several policy proposals below highlight the need for independent audits and consistent notices across ports and carriers. 4.4 Practical Implications (Biometrics). TVS use does not, on its own, increase search authority—but it affects how travelers are routed and documented. Travelers can opt out of facial capture when signage and procedures are in place but should expect manual identity checks and possible delays. In mixed carrier environments, the experience varies because signage, training, and fallback procedures differ.

5. Practical Implications for U.S. Citizens and Lawful Permanent Residents

Citizens cannot be denied entry for refusing to unlock a device, although devices may be detained. LPRs who refuse may experience delays and secondary inspections. "Basic" device searches do not need a warrant; "advanced" searches require higher approvals and, in some circuits, reasonable suspicion. Data may be copied or retained according to policy and case law. 5. Practical Implications for U.S. Citizens and LPRs — Addendum

Two core rules remain: (i) U.S. citizens must be admitted, even if they refuse to unlock a device (devices may be detained and reviewed later); (ii) LPRs who refuse may face delays and secondary inspections but still have lawful entry rights unless there are other grounds of inadmissibility. Since circuits differ on when "advanced" (forensic) device searches require reasonable suspicion, the actual risk varies by jurisdiction. Field practices also vary because supervisory approvals and "national security/immigration/customs" criteria are applied with differing levels of detail.

6. Recent Data Points

Illustrative statistics show that tens of thousands of device searches happen each year out of hundreds of millions of arrivals, which is about 0.01%. Most searches are "basic." Recent data (2024–2025): In FY2024, device searches (BSEDs) totaled 47,047; of these, 42,725 (roughly 90%) were basic, and 4,322 were advanced. CBP also reports 10,541 searches involving U.S. citizens and 36,506 involving non-U.S. citizens. With a total of 420,521,616 passengers and 12,660,784 secondary inspections, BSEDs account for about 0.3% of secondary inspections and less than 0.01% of all arrivals. CBP's public summary

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.

(FY2024) confirms 47,047 BSEDs, affecting less than 0.01% of arriving travelers, with about 90% being basic searches. U.S. Customs and Border Protection. The quarterly peak (Apr–Jun 2025): Press analysis of CBP's totals reports 14,899 device searches—the highest quarter so far. (Use cautiously; underlying CBP monthly tables inform this estimate.)

Category	Metric	Value	Unit	Period	Notes / Caveats	Primary Source (for your footnote)
Device Searches (BSED)	Total device searches	47047.0	count	FY2024	CBP-reported total border searches of electronic devices (BSEDs).	CBP FY2024 BSED report / CBP public summary
Device Searches (BSED)	Basic device searches	42725.0	count	FY2024	≈90% of total BSEDs were basic.	CBP FY2024 BSED report
Device Searches (BSED)	Advanced (forensic) device searches	4322.0	count	FY2024	Advanced extractions typically require additional approvals; circuit standards vary.	CBP FY2024 BSED report
Device Searches (BSED)	U.S.-citizen device searches	10541.0	count	FY2024		CBP FY2024 BSED report
Device Searches (BSED)	Non-U.S.-citizen device searches	36506.0	count	FY2024		CBP FY2024 BSED report
Arrivals & Secondary	Total arrivals processed	420521616.0	count	FY2024	All arriving passengers processed at ports.	CBP FY2024 report tables
Arrivals & Secondary	Secondary inspections	12660784.0	count	FY2024		CBP FY2024 report tables

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.

Derived Percentages	BSED as % of secondary inspections	0.372	%	FY2024	Calculated: Total BSED ÷ Secondary inspections × 100.	Derived from CBP FY2024 counts
Derived Percentages	BSED as % of total arrivals	0.0112	%	FY2024	Calculated: Total BSED ÷ Total arrivals × 100 (well below 0.01%).	Derived from CBP FY2024 counts
Trend (Estimate)	Quarterly device searches	14899.0	count	Apr–Jun 2025	Press estimate from CBP monthly/quarterly totals; use with caution.	Press analysis of CBP data (Q2 2025)
Biometrics	Travelers processed via facial comparison	172000000.0	count	FY2023	CBP Traveler Verification Service (TVS) deployments at air/sea/land.	CBP FY2023 biometrics overview
Biometrics	Facial comparison match rate	98.0	%	FY2023	Reported '>98%' match rate; actual testing conditions vary.	CBP FY2023 biometrics overview
Ports Operations	Total travelers processed at ports	394000000.0	count	FY2023		CBP FY2023 operations summary

7. Policy Options

Publish circuit-specific field guidance, expand ex-post auditing of advanced searches, standardize traveler notifications, increase transparency on algorithm performance and opt-outs in biometric programs, and require stronger nexus or warrants for content searches beyond contraband, depending on the circuit. 7.1 Circuit-specific field guidance and traveler notices: Publish a live, one-page matrix for officers and the public that maps controlling precedents by circuit (e.g., Cotterman/Cano vs. Alasaad) and specifies when "advanced" searches require reasonable suspicion. Pair this with uniform airport signage and carrier scripts so travelers can easily understand opt-outs and device policies. 7.2 Audit "advanced" device searches: Require post-hoc audits for every forensic extraction, with a standardized justification template, supervisory sign-off, and a quarterly public report (counts, predicates, outcomes). The goal is to ensure that "specific facts" standards are applied consistently rather than invoked generically. 7.3 Tighten retention and sharing rules: For U.S. citizens, formalize the brief COOP retention

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.

window and impose automatic deletion after case closure; for non-citizens, publish clear maximums and downstream sharing pathways. Extend the same transparency to derivative data (such as hashes and analytical work products). 7.4 Biometrics transparency. Publish independent accuracy testing (by demographic and environment), human-override statistics, and redress timelines. This directly addresses confidence gaps while maintaining throughput benefits where accuracy is strong. 7.5 Statistics with context. CBP already reports device-search volumes that are very small relative to total arrivals (~0.01%). Mandate that annual reports also break out basic versus advanced searches, predicates used, extractions retained, and suppression outcomes in subsequent prosecutions—so policymakers can see both the scale and the consequences.

8. Conclusion

Device searches at the border remain statistically rare compared to the total number of arrivals, but their impact on affected individuals can be significant. Biometric processing has expanded nationwide, primarily as a tool to improve throughput and verify identities, rather than to grant new authority for searches. The legal basis still relies on border-search case law and CBP's directive framework (Ramsey; Montoya de Hernandez; Flores–Montano; CBP Directive 3340-049A). Recent CBP reports support this baseline—most device searches are "basic," and their overall frequency is well below one-hundredth of one percent of all travelers—while DHS privacy materials (PIA-056) specify limited retention for U.S. citizens during operations (CBP FY2023/FY2024 data; DHS PIA-056).

Legally, courts agree that manual, "basic" reviews are easier for the government to justify than forensic extractions but differ on when "advanced" searches need reasonable suspicion and what criteria qualify. The Ninth Circuit's approach (Cotterman; Cano) contrasts with that of the First Circuit (Alasaad), leading to a jurisdiction-dependent risk for travelers. Practically, U.S. citizens and lawful permanent residents retain re-entry rights even if they refuse to unlock a device (though delays or device detention can occur), and facial comparison through TVS now operates across air, sea, and land with limited retention for U.S. citizens and longer retention for immigration cases (CBP Directive 3340-049A; DHS/CBP TVS materials; PIA-056).

The proposed policy plan is straightforward and ready for implementation. Circuit-specific guides and consistent traveler notices would turn doctrine into predictable practice at the border (Cotterman, Cano, and Alasaad). Post-event audits of all advanced extractions—detailing specific facts, supervisory approvals, and results—would verify whether standards are followed rather than just claimed **(CBP Directive 3340-049A)**. Clear, published retention periods (including those for derivative data, such as hashes and analytical work products) would align with **DHS statements (PIA-056**) regarding privacy outcomes. Independent reports on biometric accuracy, human-override rates, and redress timelines would make program claims verifiable. Finally, providing statistics "with context" (such as basic vs. advanced, predicates, retention outcomes, and

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.

suppression results) would help Congress and the public understand both the scope and impact **(CBP FY2023/FY2024 data).**

References:

1. CBP Directive No. 3340-049A: Border Search of Electronic Devices (January 4, 2018; updated resource page 2025).
2. United States v. Ramsey, 431 U.S. 606 (1977).
3. United States v. Montoya de Hernandez, 473 U.S. 531 (1985).
4. United States v. Flores–Montano, 541 U.S. 149 (2004).
5. United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (en banc).
6. United States v. Cano, 934 F.3d 1002 (9th Cir. 2019).
7. Alasaad v. Mayorkas, 988 F.3d 8 (1st Cir. 2021).
8. DHS/CBP Traveler Verification Service (PIA-056) and CBP Biometrics pages.
9. CBP: Border Search of Electronic Devices—FY2023 & FY2024 statistics.
10. DHS Fact Sheets (May 2023): End of Title 42 and reversion to Title 8; relevant Federal Register notices.
11. ICE Secure Communities overview; Jeh Johnson memo (Nov. 20, 2014) (PEP); EO 13768 (2017).

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.

Appendix A. Prior Draft (Verbatim)

"Detained at the Border: The Truth About Green Card Searches Under Four Presidents"

In recent years, many U.S. citizens and green card holders have found themselves subject to more invasive border checks. For many, the idea of being detained at the airport—having their phones and social media accounts searched by Customs and Border Protection (CBP) agents—has become an all-too-familiar experience. This has occurred under multiple administrations, from George W. Bush, who focused heavily on national security post-9/11, to Barack Obama, whose surveillance measures were expanded, to Donald Trump, who made visible enforcement a central issue, and finally to Joe Biden, who, despite his promises of a softer immigration approach, has continued many of the same policies.

The USA PATRIOT Act and the creation of the Department of Homeland Security (DHS) under President George W. Bush significantly expanded the authority of federal agencies, such as CBP. The border search exception rule, which allows officers to search your belongings and detain individuals without a warrant, was a tool utilized heavily during this period. Following the 9/11 attacks, there was an increasing focus on securing the U.S. borders from external threats, which led to policies that prioritized security over personal privacy.

Under Barack Obama, this surveillance expanded. Obama's DHS continued the legacy of mass surveillance, particularly through programs like Secure Communities. Though the program was meant to target violent criminals, many non-violent immigrants, including green card holders, found themselves caught in the system. Furthermore, the advent of biometric tracking and facial recognition technology enabled authorities to expand surveillance beyond borders, reaching deeply into the daily lives of travelers and immigrants.

Under Donald Trump, this surveillance was intensified and became much more visible. Trump's administration issued executive orders like Executive Order 13769 (the "Muslim Ban"), which severely restricted travel for citizens of several Muslim-majority countries. Many legal permanent residents (green card holders) were detained, their phones searched, and they were questioned at length about their political affiliations. Trump's harsh rhetoric surrounding immigration, paired with these policy shifts, made the detention of travelers more frequent and more visible. CBP officers were granted extensive powers to review social media posts, emails, and messages, all without any judicial oversight.

Joe Biden's administration, while promising a return to more humane policies, continues to uphold these surveillance practices. The use of facial recognition technology at airports has increased, and although Biden has reversed some of Trump's more aggressive policies, such as the travel bans, the reality of detentions and invasive searches

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.

for green card holders has not lessened. Title 42, a public health order allowing the expulsion of immigrants based on health risks, remains a tool of removal, and border searches continue to be a standard part of U.S. immigration enforcement.

References:

1. U.S. Customs and Border Protection. "Border Search Policies." CBP.gov.
2. The American Civil Liberties Union (ACLU). "The Expansion of Government Surveillance under Obama."
3. The Migration Policy Institute. "Immigration Enforcement and Border Search Authority." Migrationpolicy.org.
4. Executive Order 13769, "Protecting the Nation from Foreign Terrorist Entry into the United States," issued by President Donald Trump, January 27, 2017.
5. Bureau of Justice Statistics. "The Rise of Surveillance Programs in U.S. Airports." BJS.gov.

© 2025 Wardhan. Working paper distributed for scholarly and educational use. Not legal advice.